

# UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of:

3137 N. 37<sup>th</sup> Street, Milwaukee, Wisconsin and  
3137A N. 37<sup>th</sup> Street, Milwaukee, Wisconsin, more  
fully described in Attachment A

Case No. 20m807

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of:

Title 21, United States Code, Section 841(a)(1) (distribution of and possession with intent to distribute controlled substances)

The application is based on these facts: See attached affidavit.

- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



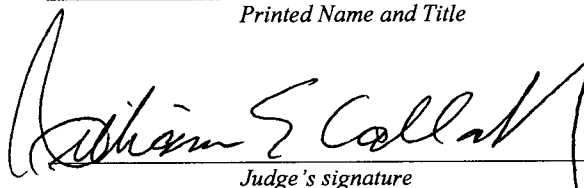
Applicant's signature

Christopher Farrell, SA

Printed Name and Title

Sworn to before me and signed in my presence:

Date: January 8, 2020



Judge's signature

City and State: Milwaukee, Wisconsin Case 20-mj-00807-WEC Filed 01/22/20 Page 1 of 33 Document 1  
William S. Callahan U.S. Magistrate Judge  
Printed Name and Title

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, Christopher Farrell, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as **3137 N. 37<sup>th</sup> Street, Milwaukee, Wisconsin, and 3137A N. 37<sup>th</sup> Street, Milwaukee, Wisconsin**, hereinafter "**PREMISES**," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the FBI and have been since August of 2008. I have been assigned to the Southeastern Wisconsin Regional Gang Task Force since September of 2019. I was previously assigned to the Louisville and Pittsburgh Field Offices. Prior to being employed with the FBI, I was a police officer for approximately six and a half years. I am an investigator or law enforcement officer of the United States within the meaning of 18 U.S.C. Section 2510(7), in that I am empowered by the law to conduct investigations of and to make arrests for federal felony arrests.

3. As a Special Agent, I have participated in the investigation of narcotics-related offenses, resulting in the prosecution and conviction of individuals and the seizure of illegal drugs, weapons, United States currency, and other

evidence of criminal activity. As a narcotics investigator, I have interviewed many individuals involved in drug trafficking and have obtained information from them regarding acquisition, sale, importation, manufacture, and distribution of controlled substances. Through my training and experience, I am familiar with the actions, habits, traits, methods, and terminology utilized by the traffickers and abusers of controlled substances. I have participated in all aspects of drug investigations, including physical surveillance, execution of search warrants, undercover operations, court-ordered wiretaps, analysis of phone and financial records, and the arrests of numerous drug traffickers. I have also been the affiant of many search warrants. Additionally, I have spoken with other experienced narcotics investigators on numerous occasions concerning the method and practices of drug traffickers and money launderers. Furthermore, I have attended training courses that specialized in the investigation of narcotics trafficking and money laundering. Through these investigations, my training and experience, and conversations with other law enforcement personnel, I have become with the methods used by drug traffickers to manufacture, smuggle, safeguard, and distribute narcotics, and to collect and launder trafficking-derived proceeds. I am further aware of the methods employed by major narcotics organizations to thwart any investigation of their illegal activities. I know that drug traffickers commonly have in their

possession, and at their residences and other locations where they exercise dominion and control, firearms, ammunition, and records or receipts pertaining to such.

4. The facts in this affidavit come my personal observations, my training and experience, my review of documents, and information obtained from other law enforcement agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

#### **PROBABLE CAUSE**

5. The United States, including the FBI and the FBI's Southeastern Wisconsin Regional Gang Task Force, are conducting a criminal investigation of ANTHONY CROSS (DOB: XX/XX/1979) regarding possible violations of Title 21, United States Code, Section 841(a)(1) (distribution of and possession with intent to distribute controlled substances).

6. In October of 2019, case agents interviewed a confidential source (CS #1). CS #1 stated that s/he bought cocaine approximately fifty times over the last two years from an individual CS #1 knows as "ANT." CS #1 indicated "ANT" sells cocaine from his house, which is located on 37<sup>th</sup> Street between Fond du Lac Avenue and Burleigh Street. According to CS #1, "ANT" is a Gangster Disciple gang

member, sometimes carries a gun, and is obtaining his cocaine from Chicago, Illinois. The CS provided a phone number of (414) 439-6701, or Target Cell Phone, for "ANT." CS #1 advised s/he could make a controlled buy of cocaine from "ANT."

7. Based upon my training and experience, I know that a "controlled buy" (and/or controlled contact) is a law enforcement operation in which a confidential source purchases drugs from a target. The operation is conducted using surveillance, usually audio and video taping equipment, and pre-recorded purchase money. When a confidential source is used, s/he is searched for contraband, weapons, and money before the operation. The confidential source is also wired with a concealed body recorder and monitoring device. When the transaction is completed, the confidential source meets case agents at a pre-determined meet location and gives the purchased drugs and the recording/monitoring equipment to the case agents. The confidential source is again searched for contraband, weapons, and money. A sample of the suspected drugs is then field tested by case agents for the presence of controlled substance and then placed in inventory pursuant to normal inventory procedures. Telephone calls to the target by the confidential source are consensually recorded calls under the direction and control of case agents and made in the presence of case agents.

8. Between November 1 and November 12, 2019, CS #1 made four controlled purchases of crack cocaine (totaling 55.29 grams) and powder cocaine (totaling 17.41 grams), from CROSS at CROSS's residence, **PREMISES**.

9. Case agents believe CS #1 is reliable and credible. First, CS #1 has provided information since October 2019. Second, CS #1's information is consistent with case agents knowledge of violent gang subjects in Milwaukee, Wisconsin and with evidence obtained elsewhere in this and other investigations where CS #1 was not utilized. Furthermore, substantial portions of CS #1's information has been corroborated by controlled drug purchases, money deliveries, consensually recorded phone calls with CROSS, as well as through independent investigation, including surveillance and information from other sources. CS #1 is cooperating with law enforcement to obtain consideration from the Milwaukee County District Attorney's Office for pending charges related to narcotics trafficking. CS #1 has prior battery, obstruction, and possession of narcotics convictions. For these reasons, case agents believe CS #1 to be reliable.

10. On November 1, 2019, case agents utilized CS #1 to conduct a controlled purchase of cocaine from "ANT." CS #1 made a consensually recorded phone call to the Target Cell Phone and told "ANT" that s/he needed to see him. "ANT" indicated "alright." Next, case agents provided CS #1 a recording device and

pre-recorded money for the controlled purchase, and then established surveillance in the area of CROSS's residence/**PREMISES**. Surveillance observed an Infiniti parked at the location and a male in a gray hood approach the vehicle, which then quickly left. Case agents believe the male had sold narcotics to the individual in the Infiniti. Shortly thereafter, case agents observed CS #1 park in the alley behind the **PREMISES**. Upon CS #1's arrival at the **PREMISES**, the same individual wearing a gray hood approached the passenger side of CS #1's vehicle, reached into the vehicle, and moments later walk back to the rear yard. After the transaction, case agents met with CS #1 and seized the crack cocaine and the recording device. Case agents field tested the crack cocaine with positive results for cocaine base and weighed approximately 6.84 grams.

11. After the controlled purchase, CS #1 was briefed. CS #1 indicated s/he called "ANT" at the Target Cell Phone and told him s/he needed seven grams. CS #1 indicated "ANT" walked up to the vehicle and gave CS #1 a knotted bag of crack cocaine. CS #1 gave \$300 in pre-recorded law enforcement funds to "ANT." CS #1 observed "ANT" walk back into the rear yard and enter the rear door at the **PREMISES**.

12. Case agents reviewed the recording device utilized by CS #1 to confirm his/her purchase of crack cocaine from "ANT."



13. On November 5, 2019, a case agent showed a single Milwaukee Police Department booking photograph of ANTHONY CROSS (DOB: XX/XX/1979) to CS #1. The photograph was unlabeled and contained no identifying information. CS #1 positively identified the photograph as the person CS #1 knew as "ANT" and the person that sold CS #1 the crack cocaine on November 1, 2019.

14. On November 5, 2019, a case agent viewed the surveillance video of the controlled narcotics purchase on November 1, 2019 and positively identified "ANT" as ANTHONY CROSS.

15. On November 6, 2019, case agents utilized CS #1 to conduct a controlled purchase of cocaine from CROSS. CS #1 made a consensually recorded phone call to the Target Cell Phone and told CROSS that s/he needed to see him. CROSS indicated "alright." After providing CS #1 with pre-recorded monies and a recording device, case agents established surveillance in the area of CROSS's residence/**PREMISES** and observed CS #1 park in the alley behind the **PREMISES**. Surveillance observed CROSS walk to the front yard of the address and approach a vehicle. CROSS entered the vehicle and exited moments later. Shortly thereafter, surveillance observed CROSS walk to the back yard and approach CS #1's vehicle on the passenger side. Moments later, CROSS walked back to the back yard and was then observed in the front yard entering the



previously observed vehicle. After the transaction, case agents met with CS #1 and seized the cocaine and the recording devices. Case agents field tested the cocaine with positive results for cocaine base and weighed approximately 13.94 grams.

16. After the controlled purchase, CS #1 was briefed. CS #1 indicated s/he called CROSS at the Target Cell Phone and told him s/he needed "half of soft." According to CS #1, CROSS walked up to the passenger side of the vehicle and gave CS #1 a paper ball filled with cocaine. CS #1 gave CROSS \$600 in pre-recorded law enforcement funds.

17. Case agents reviewed the recording device utilized by CS #1 to confirm his/her purchase of cocaine from CROSS. A case agent viewed the surveillance video of the controlled narcotics purchase and positively identified the individual giving the narcotics to CS #1 as CROSS.

18. On November 6, 2019, I met with CS #1 who indicated s/he had purchased approximately one kilogram of powder cocaine from CROSS since 2012 or 2013. CS #1 stated CROSS is a Gangster Disciple and overheard him state he had relatives who are 4 Corner Hustlers in Chicago. CS #1 believed CROSS is obtaining his narcotics from these individuals in Chicago.

19. On November 12, 2019, case agents utilized CS #1 to conduct a controlled purchase of cocaine from CROSS. CS #1 made a consensually recorded

phone call to the Target Cell Phone, and CROSS told CS #1 he would call CS #1 back. CROSS, using the Target Cell Phone, called back and indicated he was “over there,” and CS #1 stated s/he would be there in a minute. CS #1 then drove to the **PREMISES** equipped with a recording device and pre-recorded law enforcement monies.

20. Case agents established surveillance in the area of the **PREMISES** and observed CS #1 park in the alley behind the **PREMISES**. Surveillance observed CROSS walk to CS #1’s driver side door and return to the rear of the residence. Shortly thereafter, CROSS returned to the driver’s side door and then quickly ran back to the rear yard of the residence. After the transaction, case agents met with CS #1 and seized the cocaine and the recording device. Case agents field tested the cocaine with positive results for cocaine base and powder cocaine. The crack cocaine weighed 41.53 grams and the powder cocaine weighed 3.47 grams.

21. After the controlled purchase, CS #1 was briefed. CS #1 indicated s/he called the Target Cell Phone and told CROSS s/he needed an ounce and one-half of crack cocaine and a ball of powder cocaine. CROSS met CS #1 at the driver door and gave CS #1 one-half ounce of crack cocaine. CS #1 told CROSS he wanted an ounce and one-half of crack cocaine and a ball of powder cocaine. CROSS told CS #1 he thought s/he only wanted a half. CS #1 gave CROSS \$1,950 in cash. CROSS

returned and gave CS #1 a bag with an ounce of crack cocaine and another bag with a ball of powder cocaine.

22. Case agents reviewed the recording device utilized by CS #1 to confirm his/her purchase of cocaine from CROSS. A case agent viewed the surveillance video of the controlled narcotics purchase and positively identified the individual giving the narcotics to CS #1 as CROSS.

23. On December 4, 2019, a U.S. Magistrate Judge in the Eastern District of Wisconsin signed a search and seizure warrant to obtain prospective E-911/GPS Data latitude-longitude information for the Target Cell Phone. The U.S. Magistrate Judge also signed a pen register trap and trace order for the Target Cell Phone.

24. On December 11, 2019, case agents utilized CS #1 to conduct a controlled purchase of cocaine from CROSS. CS #1 made a consensually recorded phone call to the Target Cell Phone and CROSS told CS #1 to "come through there." CS #1 then drove to the **PREMISES** equipped with a recording device and pre-recorded law enforcement monies.

25. Case agents established surveillance in the area of the **PREMISES** and observed CS #1 park in the alley behind the **PREMISES**. Surveillance observed CROSS walk to CS #1's passenger door and then return to the rear of the residence. CS #1 exited the vehicle and walked to the front passenger door, reached

into the vehicle, and then returned to the driver seat. After the transaction, case agents met with CS #1 and seized crack cocaine and the recording device. Case agents field tested the crack cocaine with positive results for cocaine. The crack cocaine weighed 6.92 grams.

26. After the controlled purchase, CS #1 was briefed. CS #1 indicated s/he called the Target Cell Phone once he arrived in the alley behind the **PREMISES** and told CROSS s/he needed "7 hard." CROSS met CS #1 at the passenger door and CS #1 gave CROSS \$300. CROSS then dropped a corner cut bag of crack cocaine on the front passenger seat. The bag fell between the front seat and the passenger door. CROSS then walked back into the rear of the **PREMISES**. CS #1 exited the vehicle and walked over to the front passenger seat to pick up the crack cocaine.

27. Case agents reviewed the recording device utilized by CS #1 to confirm his/her purchase of cocaine from CROSS. A case agent viewed the surveillance video of the controlled narcotics purchase and positively identified the individual giving the narcotics to CS #1 as CROSS.

28. Case agents reviewed the location data for the Target Cell Phone during the purchase of crack cocaine from CROSS on December 11, 2019. The crack cocaine purchase occurred between approximately 12:15PM and 12:21PM. The location data showed the Target Cell Phone within 9 meters of the **PREMISES** at

approximately 11:58AM, within a 121 meter radius of the **PREMISES** at approximately 12:13PM, and within an 8 meter radius of the **PREMISES** at approximately 12:28PM. Case agents reviewed pen register trap and trace data for the Target Cell Phone, which showed CS #1 making a phone call to CROSS at approximately 12:07PM and another call at approximately 12:15PM.

29. On December 22, 2019, law enforcement conducted physical surveillance at the **PREMISES**. At approximately 4:45PM, a case agent observed two vehicles parked in the alley behind the **PREMISES**, in the same manner CS #1 would park in the alley to purchase narcotics. The case agent observed an unidentified individual approach both vehicles briefly and then return to a location that appeared to be the **PREMISES**.<sup>1</sup> Based upon their training, experience, and familiarity with this investigations, case agents believed both vehicles just engaged in a narcotics transaction with the subject, who was believed to be CROSS.

30. The Milwaukee Police Department conducted a traffic stop on one of the vehicles, a Chevrolet Malibu, shortly after leaving the area. The police officer detected a strong odor of marijuana coming from the vehicle, and observed marijuana in the vehicle. The individual was detained in handcuffs and then fled

---

<sup>1</sup> Because it was dark outside, the individual was not able to be positively identified.

on foot from the police officer, but subsequently caught. A police canine positively alerted on the vehicle. A subsequent search of the vehicle resulted in locating a hidden compartment behind the center display screen which contained nine Oxycodone Hydrochloride, 20 milligram pills. A .40 caliber firearm fully loaded with an extended 30-round capacity magazine was located underneath the driver's seat. Approximately 501.8 grams of marijuana was also seized from a backpack in the vehicle. The individual provided a mirandized interview and claimed he purchased the narcotics from a guy named "Tay" near 15<sup>th</sup> and North Avenue for \$1,500. The individual also indicated he bought the gun because of the marijuana in the car.

31. The Milwaukee Police Department conducted a traffic stop on the second vehicle observed during the surveillance, a Nissan Altima. The driver had an active arrest warrant and was placed into custody. A search incident to arrest located a bag of marijuana in the individual's interior left jacket pocket and weighed approximately 6.90 grams. The individual provided a mirandized interview but did not indicate from whom he bought the marijuana.

32. Case agents reviewed the location data for the Target Cell Phone during the surveillance of the **PREMISES** on December 22, 2019 at approximately

4:45 p.m. The location data indicated the Target Cell Phone was within a 719 meter radius of the **PREMISES** at 4:29 p.m., 4:44 p.m., and 5:00 p.m.

33. Case agents reviewed the location data for the Target Cell Phone and observed on December 29, 2019 at approximately 2:44 p.m., the Target Cell Phone traveled to the Wisconsin/Illinois border on Highway 94 and stayed in a remote location for over an hour. CS #1 previously indicated CROSS may be obtaining his narcotics from the Chicago area. Case agents believe this may have been CROSS obtaining narcotics from his supplier in Chicago.

34. On January 3, 2020, case agents conducted a database check on the City of Milwaukee website for property information for the **PREMISES**. The check revealed the property has two units: **3137A N. 37<sup>th</sup> Street** and **3137 N. 37<sup>th</sup> Street**. The property owner for both units is Dianne Cross, believed to be CROSS' mother. Case agents conducted a utilities check with Wisconsin Energies for the **PREMISES**. Dianne Cross, believed to be CROSS' mother, was listed on the account for the lower unit since April 14, 2014. Shanella Washington was listed on the account for the upper unit since June 6, 2019.

35. CS #1 advised case agents that CROSS lives in the upper unit of the **PREMISES** with two or three children, but that CS #1 has never been in the



house. Having never been in the residence, CS #1 could not provide additional information regarding the inside layout of the residence.

36. Law enforcement database reflects that CROSS is associated with both units at this address, **3137A and 3137 N. 37<sup>th</sup> Street**. Additionally, in October 2014, Milwaukee Police Department reported to a burglary complaint that occurred at 3137 N. 37<sup>th</sup> Street (**PREMISES**), at which time CROSS occupied the upper unit. The first floor of the property was under construction and not occupied. At this time, CROSS told police that he was renovating the home for his mother, Diane Cross, who is the owner of the entire building.

37. Therefore, based upon the CS's statement, law enforcement databases, and CROSS' familial relationship with Dianne Cross, case agents believe CROSS has access to both units.

#### **TECHNICAL TERMS**

41. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be

assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

42. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **PREMISES**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive, cellular telephone, or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage

media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

43. *Probable cause.* I submit that if a computer, cellular telephone, or storage medium is found on the **PREMISES**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

44. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **PREMISES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted

portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage

media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of

additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the



computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

45. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

46. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

47. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

### CONCLUSION

48. I submit that this affidavit supports probable cause for a warrant to search the **PREMISES** described in Attachment A and seize the items described in Attachment B.

## **ATTACHMENT A**

### **Property to be searched**

**3137 N. 37<sup>th</sup> Street, Milwaukee, Wisconsin and 3137A N. 37<sup>th</sup> Street, Milwaukee, Wisconsin**, to include all associated vehicles (registered to 3137 N. 37<sup>th</sup> Street and 3137A N.37<sup>th</sup> Street) parked on the premises, basement, storage and garage areas controlled by ANTHONY CROSS. This address is further described as a two-story residence having yellow brick siding with white trim around the windows and dark colored shingles. The second level also has a living area that has two side windows and contains off-white siding. To the left of the front door to the residence has the numbers "3137" affixed in black lettering. To the left of the front window of the residence, near the side walkway, are the numbers "3137A" in black lettering which is affixed to the brick. The walkway leads to a side door with an off-white awning. The backyard has a white privacy fence.



## ATTACHMENT B

### Property to be seized

1. Evidence, fruits, and instrumentalities of violations of Title 21, United States Code, Section 841(a)(1) (Distribution and possession with intent to distribute controlled substances), those violations involving ANTHONY CROSS, including:
  - a. Controlled substances, controlled substance analogues, or listed chemicals;
  - b. Paraphernalia associated with the manufacture and distribution of controlled substances including but not limited to materials and items used for packaging, processing, diluting, weighing, and distributing controlled substances, such as scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, and heat-sealing devices;
  - c. Duffel, canvas bags, suitcases, safes, or other containers to hold or transport controlled substances and drug trafficking related items and proceeds;
  - d. Proceeds of drug trafficking activities, such as United States currency, precious metals, financial instruments, and jewelry, and documents and deeds reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry or other items obtained with the proceeds from drug trafficking activities;
  - e. Firearms, ammunition, magazines, gun boxes, firearm purchase records or receipts, and other paraphernalia associated with firearms;
  - f. Bank account records, loan documents, wire transfer records, money order receipts, postal express mail envelopes, bank statements, safe deposit box keys and records, money containers, financial records and notes showing payment, receipt, concealment, transfer, or movement of money generated from the sale of controlled substances, or financial transactions related to the trafficking of controlled substances;



- g. Drug or money ledgers, drug distribution or customer lists, drug supplier lists, correspondence, notations, logs, receipts, journals, books, records, and other documents noting the price, quantity, and/or times when controlled substances were obtained, transferred, sold, distributed, and/or concealed;
- h. Personal telephone books, address books, telephone bills, photographs, letters, cables, telegrams, facsimiles, personal notes, receipts, documents and other items or lists reflecting names, addresses, purchases, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in drug trafficking activities;
- i. Records of off-site storage locations, including but not limited to safe deposit box keys and records, and records and receipts and rental agreements for storage facilities;
- j. Cellular telephones, Smartphones, text messaging systems, and other communication devices, and all electronic storage areas on the device including stored telephone numbers, recently called numbers list, text messages, digital audio and/or video recordings, pictures, settings, and any other user defined settings and/or data, as well as any records associated with such communications services used to commit drug trafficking offenses;
- k. Records, items and documents reflecting travel for the purpose of participating in drug trafficking activities, such as passports, airline tickets, bus tickets, vehicle rental receipts, credit card receipts, taxi cab receipts, hotel and restaurant receipts, canceled checks, maps, and records of long distance calls reflecting travel;
- l. Indicia of occupancy, residency or ownership of the premises and things described in the warrant, including utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents and keys;
- m. Photographs, videotapes or other depictions of assets, firearms, coconspirators, or controlled substances; and

2. Computers, cellular telephones, or storage media used as a means to commit the violations described above;

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- c. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

- i. records of or information about Internet Protocol addresses used by the COMPUTER;
- j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- k. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order

to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.